Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) A computer platform having:

a trusted module which is resistant to internal tampering and which stores a third party's public key certificate;

means storing license-related code comprising at least one of a secure executor for checking whether the platform or a user thereof is licensed to use particular data and for providing an interface for using the data and/or for monitoring its usage, and a secure loader for checking whether the platform or a user thereof is licensed to install particular data and/or for checking for data integrity before installation, the license-related code including secure key-transfer code for enabling a license key to be transferred between the trusted module and a further trusted module of another computer platform; ~~and~~

means storing a hashed version of the license-related code signed with the third party's private key; and

means for integrity checking the license-related code with reference to the signed version and the public key certificate and preventing the license-related code from being loaded if the integrity check fails.

2. (previously presented) A computer platform as claimed in claim 1, wherein the means for integrity checking further comprises:

means for reading and hashing the license-related code to produce a first hash;

means for reading and decrypting the signed version using the public key certificate to produce a second hash; and

means for comparing the first and second hashes.

3. (canceled)

4. (previously presented) A computer platform as claimed in claim 1, wherein the license-related code also includes a library of interface subroutines which can be called in order to communicate with the trusted module.

5. (previously presented) A computer platform as claimed in claim 1, wherein the license-related code includes, for at least one group of data, a (or a respective) software executor which specifies the respective group of data and which is operable to act as an interface to that group of data.

6. (previously presented) A computer platform as claimed in claim 1, wherein the means storing the license-related code and/or the means storing the hashed version of the license-related code are provided, at least in part, by the trusted module.

7. (currently amended) A computer platform ~~as claimed in claim 1,~~ comprising:

a trusted module which is resistant to internal tampering and which stores a third party's public key certificate;

means storing license-related code comprising at least one of a secure executor for checking whether the platform or a user thereof is licensed to use particular data and for providing an interface for using the data and/or for monitoring its usage,

and a secure loader for checking whether the platform or a user thereof is licensed to install particular data and/or for checking for data integrity before installation;

means storing a hashed version of the license-related code signed with the third party's private key; and

means for integrity checking the license-related code with reference to the signed version and the public key certificate and preventing the license-related code from being loaded if the integrity check fails;

wherein the trusted module and an operating system of the platform have a dedicated communications path therebetween which is inaccessible to other parts of the computer platform.

8. - 18. (cancelled)

19. (currently amended) A computer platform ~~as claimed in claim 5,~~ comprising:

a trusted module which is resistant to internal tampering and which stores a third party's public key certificate;

means storing license-related code comprising at least one of a secure executor for checking whether the platform or a user thereof is licensed to use particular data and for providing an interface for using the data and/or for monitoring its usage, and a secure loader for checking whether the platform or a user thereof is licensed to install particular data and/or for checking for data integrity before installation, wherein the license-related code includes, for at least one group of data, a (or a respective) software executor which specifies the respective group of data and which is operable to act as an interface to that group of data;

means storing a hashed version of the license-related code

signed with the third party's private key; and

means for integrity checking the license-related code with reference to the signed version and the public key certificate and preventing the license-related code from being loaded if the integrity check fails; and wherein:

the software executor (or at least one of the software executors) contains a public key of the trusted module and a licensing model for the respective data;

the platform includes an operating system that is operable to request ~~that~~ the software executor that its respective data be used;

in response to such a request, that software executor is operable to request the secure executor to license-check, using its licensing model, whether the platform or a user thereof is licensed to use that data;

in response to such latter request, the secure executor is operable to perform the requested license-check, to sign the result of the license check using a private key of the trusted module, and to respond to that software executor with the signed result; and

in response to such a response, that software executor is operable:

to check the integrity of the signed result using the public key of the trusted module; and

upon a successful integrity check of a successful license-check result, to request the operating system to use that data.

20. (currently amended) A computer platform ~~as claimed in claim 5,~~ comprising:

a trusted module which is resistant to internal tampering

and which stores a third party's public key certificate;

means storing license-related code comprising at least one of a secure executor for checking whether the platform or a user thereof is licensed to use particular data and for providing an interface for using the data and/or for monitoring its usage, and a secure loader for checking whether the platform or a user thereof is licensed to install particular data and/or for checking for data integrity before installation, wherein the license-related code includes, for at least one group of data, a (or a respective) software executor which specifies the respective group of data and which is operable to act as an interface to that group of data;

means storing a hashed version of the license-related code signed with the third party's private key; and

means for integrity checking the license-related code with reference to the signed version and the public key certificate and preventing the license-related code from being loaded if the integrity check fails; and wherein:

the software executor (or at least one of the software executors) contains a public key of the trusted module and a licensing model for the respective data;

the platform includes an operating system that is operable to request ~~that~~ the software executor that its respective data be used;

in response to such a request, the secure executor is operable to send to the respective software executor a request, signed using a private key of the trusted module, for a licensing model for the particular data;

in response to such latter request, that software executor is operable:

to check the integrity of the request using the public

key of the trusted module; and

upon a successful integrity check, to send the licensing model to the secure executor; and

upon receipt of the licensing model, the secure executor is operable:

to perform a license-check using that licensing model; and

upon a successful license-check result, to request the operating system to use that data.

21. (previously presented) A computer platform as claimed in claim 1, wherein:

the secure executor contains at least one licensing model;

the operating system is operable to request the secure executor that particular data be used; and

in response to such a request, the secure executor is operable:

to perform a license-check using the, or one of the, licensing models; and

upon a successful license-check, to request the operating system to use that data.

22. (previously presented) A computer platform as claimed in claim 21, wherein the operating system is programmed to use the particular data only in response to the secure executor or the software executor.

23. - 25. (cancelled)

26. (previously presented) A computer platform as claimed in claim 21, wherein the trusted module is operable to log the

request to the operating system to use the data.

27. (currently amended) A computer platform ~~as claimed in claim 21,~~ comprising:

a trusted module which is resistant to internal tampering and which stores a third party's public key certificate;

means storing license-related code comprising at least one of a secure executor for checking whether the platform or a user thereof is licensed to use particular data and for providing an interface for using the data and/or for monitoring its usage, and a secure loader for checking whether the platform or a user thereof is licensed to install particular data and/or for checking for data integrity before installation, the secure executor containing at least one licensing model;

means storing a hashed version of the license-related code signed with the third party's private key; and

means for integrity checking the license-related code with reference to the signed version and the public key certificate and preventing the license-related code from being loaded if the integrity check fails; wherein

the platform includes an operating system that is operable to request the software executor that its respective data be used; and

in response to such a request, the secure executor is operable:

to perform a license-check using the, or one of the, licensing models; and

upon a successful license-check, to request the operating system to use that data;

the platform further including a further, removable, trusted module containing a user identity;

wherein the platform is operable to perform an authentication check between the first-mentioned trusted module and the removable trusted module; and

wherein, upon license license-checking, the secure executor or software executor is operable to perform the license-check with reference to the user identity.

28. (canceled)

29. (currently amended) A computer platform having:

a trusted module which is resistant to internal tampering and which stores a third party's public key certificate;

means storing license-related code comprising, for at least one group of data, a (or a respective) software executor which specifies the respective group of data and which is operable to act as an interface to that group of data, the license-related code further comprising at least one of:

a secure executor for checking whether the platform or a user thereof is licensed to use particular data and for providing an interface for using the data and/or for monitoring its usage; ~~and~~

a secure loader for checking whether the platform or a user thereof is licensed to install particular data and/or for checking for data integrity before installation; and

means storing a hashed version of the license-related code signed with the third party's private key;

wherein the computer platform is programmed so that, upon booting of the platform:

the license-related code is integrity checked with reference to the signed version and the public key certificate; and

if the integrity check fails, the license-related code is prevented from being loaded; and

wherein the means storing the license-related code and/or the means storing the hashed version of the license-related code are provided, at least in part, by the trusted module; and further wherein

the software executor (or at least one of the software executors) is operable to request the trusted module to install particular data;

in response to such a request, the secure loader within the trusted module is operable to license-check whether the platform or a user thereof is licensed to install that particular data and/or to check the integrity of that data and to respond to the operating system with the result of the check; and

in dependence upon the response, the operating system is operable to install or not to install the particular data.

30. (canceled)

31. (currently amended) A computer platform as claimed in claim 29, wherein the platform includes an operating system ~~is~~ programmed to install the particular data only in response to the trusted module.

32. (currently amended) A computer platform as claimed in claim ~~30~~ 29, wherein the trusted module and an operating system of the platform have a dedicated communications path therebetween which is inaccessible to other parts of the computer platform, and wherein the response from the trusted module to the operating system is supplied via the dedicated communications path.

33. (previously presented) A computer platform as claimed in claim 29, wherein, if the check succeeds, the trusted module is operable to generate a log for auditing the particular data.

34. (previously presented) A computer platform as claimed in claim 29, wherein, if the check succeeds, the secure loader is operable to perform a virus check on the particular data.

35. (previously presented) A computer platform as claimed in claim 29, wherein, upon installation, the particular data is installed into the trusted module.

36. (previously presented) A computer platform as claimed in claim 29:

further including a further, removable, trusted module;

wherein the platform is operable to perform an authentication check between the first-mentioned trusted module and the removable trusted module; and

wherein, upon installation, the particular data is installed into the further trusted module.

37. (currently amended) A computer platform as claimed in claim 29, wherein:

the secure executor contains at least one licensing model;

the software executor (or at least one of the software executors) is operable to request the trusted module that ~~is~~ its respective data be used;

in response to such a request, the secure executor within the trusted module is operable:

to perform a license-check using the, or one of the, licensing models; and

upon a successful license-check, to request the operating system to use that data.

38. (previously presented) A computer platform as claimed in claim 37, wherein the operating system is programmed to use the particular data only in response to the trusted module.

39. (previously presented) A computer platform as claimed in claim 37, wherein the trusted module and an operating system of the platform have a dedicated communications path therebetween which is inaccessible to other parts of the computer platform, and wherein the request from the secure executor to the operating system to use the data is supplied via the dedicated communications path.

40. (previously presented) A computer platform as claimed in claim 37, wherein the trusted module is operable to log the request to the operating system to use the data.

41. (previously presented) A computer platform as claimed in claim 37;

further including a further, removable, trusted module containing a user identity;

wherein the platform is operable to perform an authentication check between the first-mentioned trusted module and the removable trusted module; and

wherein, upon license-checking, the secure executor or software executor is operable to perform the license-check with reference to the user identity.

42. (previously presented) A computer platform as claimed in

claim 19, wherein the operating system is programmed to use the particular data only in response to the secure executor or the software executor.

43. (previously presented) A computer platform as claimed in claim 19, wherein the trusted module is operable to log the request to the operating system to use the data.

44. (previously presented) A computer platform as claimed in claim 19;

further including a further, removable, trusted module containing a user identity;

wherein the platform is operable to perform an authentication check between the first-mentioned trusted module and the removable trusted module; and

wherein, upon license-checking, the secure executor or software executor is operable to perform the license-check with reference to the user identity.

45. (previously presented) A computer platform as claimed in claim 20, wherein the operating system is programmed to use the particular data only in response to the secure executor or the software executor.

46. (previously presented) A computer platform as claimed in claim 20, wherein the trusted module is operable to log the request to the operating system to use the data.

47. (previously presented) A computer platform as claimed in claim 20;

further including a further, removable, trusted module

containing a user identity;

wherein the platform is operable to perform an authentication check between the first-mentioned trusted module and the removable trusted module; and

wherein, upon license-checking, the secure executor or software executor is operable to perform the license-check with reference to the user identity.